I-SUITE QUICK START GUIDE

For Nevada Type 3 IMT's

04/23/2009

Table of Contents:

1. Computer Set-up:

Each team has 4 laptop computers labeled:
SERVER
WORKSTATION1
WORKSTATION2
WORKSTATION3

The SERVER computer is the machine where all of the ISUITE database information and other team data will be stored. The client computers or WORKSTATIONS will communicate with the SERVER to access this information. This access is made possible via the wireless router provided for each team to use. For help with your wireless router see the WIRELESS Guide. The server computer can access and manipulate the ISUITE data without any connection present as the database is stored locally on the SERVER. However the WORKSTATIONS must be connected to the network in order to access the database.

Upon arriving at an indent select a suitable location to set-up the computers. Consider environmental factors that may affect the laptops as well as other electronic equipment when choosing your location. Avoid locations with high levels of moisture or humidity, temperature extremes (hot or cold), or areas where dust might be a factor. Select a location where adequate workspace, lighting, and power outlets are available. Consider that each laptop, the printer, the wireless router, and any additional office machines (printers, copiers, etc.) will need to be plugged in to a power outlet.

*Please note: You do not have to set-up all of the workstation computers. In some situations it may only be necessary to use the sever computer with no workstations or wireless router. This is especially true at your initial arrival at the incident where your priorities may be simply to set-up the database, check-in resources, and develop your first shift's IAP. Workstations can be added later as the need arises. In most cases the Plans Section Chief and Finance Section Chief will require their own dedicated computer. It is acceptable to do your work on the SERVER computer as long as you pause to allow it to complete its scheduled backups.

Here is the proper order to power-on and connect your Teams devices.

1. Plug-in your wireless router and allow it approximately 1 minute to become ready to accept connections and begin transmitting data.

2. Unpack and plug-in the computer marked SERVER and power it on
3. At the login window type your username and password (see passwords file)
4. Ensure that you are connected to your wireless router by checking the wireless icon at the bottom right corner of the notification area on the taskbar. This connection should happen automatically. For help see the wireless guide.
5. Start the ISUITE application and set-up your database. The procedures to do this depend on the type of incident, rather it is a new incident or you are taking over from another team. Consult the database section on page 11 of this guide on how to do this.
6. Once your database is created or restored enter the incident data under the DATA ADMIN module. For instructions on how to do this see page 11 of this guide.
7. Once the data is input into the database it is time to do the ROSS data import. For instructions on how to do this consult page 12 of this guide.
8. Now your ISUITE database should be ready to put into production.
9. Before connecting clients it is a good time to set-up a shared printer
10. For instruction on how to install and share a printer consult the documentation included with your particular printer. I advise connecting the printer directly to the server computer via a USB cable. Install the driver software that came with your printer and ensure that you are able to print a test page from the server computer.
11. To simply share the printer navigate to Start > Printers and Faxes
12. Right-Click on the printer you just installed and click Sharing…
13. Click the radio button for Share this printer
14. Give the printer a share name and click OK
15. Notice how the printer is now displayed with a hand under it signifying that the printer is shared.
16. Close the printers window
17. It is now time to set-up and connects your WORKSTATIONS.
18. Unpack the WORKSTATION computers connect them to power and power them on
19. At the login window type the username and password. (See the password file).
20. Ensure that all workstations are connected to your wireless router by checking the wireless icon at the bottom right corner of the notification area on the taskbar. This connection should happen automatically. For help see the wireless guide.

2. Networking:

All team laptops are configured to automatically connect to that team's wireless router whenever it is in range. Consult the wireless guide if one or all of your machines are unable to connect. When all of your machines are connected they will share access to the ISUITE Database, Shared Team Folder found on the desktop, an Internet connection (if available), and any shared printers (if available).

Each team's computers are configured with certain network attributes specific to that team. These include a unique block of IP addresses assigned by the router that will allow up to 10 computers to communicate simultaneously on the network. These addresses are assigned via the router and no manual IP addressing is necessary. Also each team's laptops have been placed into a team specific WORKGROUP that will allow them to share resources with each other but not with any other networks or computers.

Each team's laptops may be either connected wirelesses using the provided team routers (this is the preferred connection method) or via 10/100 network cards built into the laptops using Ethernet cables and the 4 Ethernet ports on the back of the router or some other 10/100 Ethernet hub or switch.

*Please note that the routers are configured as password protected to ensure that unauthorized wireless clients do not gain access to the ISUITE data or other team resources. Additionally all of the wireless communications are encrypted for added security. All of the computers are configured with a software firewall and anti-virus / anti-spyware protection for added security.

Each of the computers has a 'Shared Team Folder' on the desktop. These folders allow for files and data to be shared across the network with the other computers. Use these folders to store narratives, write-ups, and any other important data. The contents of this folder are physically stored on the Server computer and is then made accessible by all team computers in that workgroup. This data should be burned to a CD along with the I-Suite database and turned over at the close of the incident with the final package.

In order to gain internet access you may need to plug an internet enabled Ethernet cable into the port labeled WAN on the back of your router. The router should configure this connection automatically and then share it with all your team laptops. Consult the router documentation in the resources folder for more information.

In some cases you may be using a router other the team router provided to you to connect your laptops. This is common if you are working out of contracted

communications trailer or are receiving satellite internet services from a contracted vendor. Your laptops are configured to obtain IP address automatically from a router and may not work if this service is not available on the router you are using. You may need to work with the vendor to configure your computers to establish a connection to their particular system. **Please be sure to undo any changes that you make at the end of the incident to ensure that you are able to use your team routers again.**

3. Password an Naming Conventions:

For a complete list of your teams Computer, Router, I-SUITE, and other application passwords consult the 'Passwords' file in the Resources Folder. All I-Suite passwords must meet the following criteria:

- Passwords must be 12 Characters
- Must contain capital and lowercase letters (A – Z)
- Must contain a Number (0-9)
- A Special Character (! # % & * _)
- Cannot be a dictionary word
- Once a password is change the last 5 passwords may not be reused

This criterion applies to both the ISUITE user passwords as well as the database password. All I-Suite users should be preset-up for you when you create a new incident database. Review the Password file for a complete list.

When naming incident database please use the following conventions. Incident Name with the first letter capitalized. , followed by the year, and !. Ensure that this name meets the 12 character minimum requirement. You may need to add additional characters to meet these criteria. If the fire name contains two words such as; Big Fire, eliminate any spaces.
Example: Bigfire2009!

This database name will also be set as the database password. This makes it easy to remember the password as you then only need to look at the name to know the password.

*Please Note: Any user can change their passwords from the tools menu > change password. If your password is reset by a database admin user this password is only temporary and must be reset the first time you log in. User accounts will lock after 3 failed log-in attempts. They must then be unlocked by a database admin user. The password for any user account will expire 60 days from the last time it was set or reset. You will begin receiving messages that your password will expire 3 day prior to the expiration date. If the admin user cannot access the database you must contact the ISUITE helpdesk.

To create user accounts open the Database Admin module and click users. Click the Add button at the bottom of the User Management window. Fill-in all required information and make sure all checkboxes are checked to make a user active and have all rights. **If you do** create new users or reset passwords be sure to update your Passwords file in the resources folder.

4. The 'SERVER':

This computer is where all of the ISUITE and other team data is stored. This computer then serves that data to the WORKSTATIONS that connect to it. It holds the ISUITE database as well as the data stored in the shared team folder. As suggested in the COMPUTER SETUP section of this document it may also act as the print server for your workgroup. The SERVER computer is the only machine that has the ISUITE database service running by default and therefore it must be turned on and connected to the network before the WORKSTATION computers will be able to gain access to the ISUITE database or shared team resources. The server is also the computer responsible for performing database back-ups and storing repository data files.

To login to ISUITE on the SERVER computer type in the username and password of the Admin User (see Password file). Set the Server field as (LOCAL)\ISUITE2. Leave the database field blank. In order for others to login to the ISUITE application the SERVER must remain on and running at all times.

*Please Note: The WORKSTATION computers will still be able to access the ISUITE database even if the ISUITE application is closed on the SERVER computer. No user needs to be logged in at the SERVER, the SERVER needs only be turned on, connected to the network to share the ISUITE database with other users.

5. The 'WORKSTATIONS':

There are 3 computers labeled as WORKSTATION1, WORKSTATION2, and WORKSTATION3. These computers **DO NOT** store any important data, they access shared data and resources by connecting to the SERVER computer. This includes data in the Shared Team Folder, I-Suite databases, and printers. In order to gain access to these resources the SERVER computer must be on and connected to the network. In addition, the WORKSTATION computers attempting to access these resources must have a network connection.

To login to ISUITE on the WORKSTATION computers type in a username and password from the Password file. Set the Server field as SERVER\ISUITE2. Set the database field as the name of the database you wish to connect to. In order for workstations to login to the ISUITE application the SERVER must remain on and running at all times and connected to the network. You will notice that because the clients must continually communicate with the SERVER in order to access and manipulate data you will see more of a lag in ISUITE operations than you would if you were using the SERVER computer. The same is also true if the SERVER is performing database backups or if all the clients are working in the database at the same time. Additionally as the database becomes larger the speed of the ISUITE application will decrease.

*Please Note: users are only allowed to have one connection to the database at a time. This means that if a user is already connected to the database on WORKSTATION1 then that same user account may not be used to login on WORKSTATION2.

6. Getting Help:

There are a variety of resources available to assist you, if you need help.

- Review the documents in the resources folder on your computers desktop. There you will find the ISUITE User guides, Password file, Wireless Guide, Router Documentation, and Quick Start Guide
- Review resources in the Type 3 folder
- Use Help with in the ISUITE application by selecting help from the main menu
- Contact the ROSS / ISUITE Helpdesk @ 866-224-7677 or via email helpdesk@dms.nwcg.gov
- Visit the ISuite or Ross websites:
  - http://isuite.nwcg.gov ISUITE
  - http://ross.nwcg.gov ROSS
- For FAM Web Help visit their website at: http://fam.nwcg.gov/fam-gov/ or call 800-253-5559
- For GIS Help / Support Contact Amanda Kriwox akriwox@fs.fed.us or phone (208) 420-5788
- For computer / ISUITE support contact Josh Nicholes jnicholes@fs.fed.us or phone (775) 296-0269

7. Create a New Incident:

To create a new incident database for an incident Login to the ISUITE application on the SERVER computer as the Master Admin User (see passwords file). Be sure the Server Box is set to (LOCAL)\ISUITE2 and the Database box is blank. Open the Database Admin Module.

1. Click Copy / New DB
2. Click the Browse Button (…)
3. Double click Masterdb2009!.mdf.gpg
4. Under Database password enter Masterdb2009!
5. Give the database the proper name and password using the naming convention on page 7 of this guide.
6. Click OK; the database will be automatically attached
7. Open the Data Admin module
8. Enter Incident Name
9. Enter Incident #
10. Enter Location
11. Enter State
12. Enter the date the fire started (Not necessarily the same as the day your team got there)
13. Enter Default accounting code information
14. Click Save
15. Click Accounting Codes on the left hand side
16. Enter additional accounting codes one at a time clicking save after each one
17. Click Close

*Note most of this information is found at the top of your resource order.

To restore an Incident Database from a backup file see page 16 of this guide.

8. Performing the ROSS Import:

The ROSS data import is a mechanism to populate your ISUITE incident database with resources already ordered for your incident via the ROSS system. This will save you having to enter those resources manually using the Resources tab in ISUITE. It is advisable to download the ROSS import file prior to arriving at the incident either at your home office or from the office / dispatch center where you receive your in-brief. This data is updated in real time so it is advisable to try and obtain the most recent copy of the import file as possible. Download the file from any internet connected computer and save it to a portable thumb drive or CD-R. You will need the incident number for your incident. This information is located on your resource order.

1. Navigate to http://rossreports.nwcg.gov/cognos/c8/cgi-bin/cognos.cgi
2. Select Namespace ROSSLDAPSSL and Click OK
3. Enter your ROSS Import Password (see Password file) Click OK
4. Under the Public Folders Tab Click ROSS
5. Click User Community Reports
6. Click System Extracts
7. Click I-SUITE Import File
8. Click on Incident on the top left side of the page
9. Use the Incident Text boxes to search for your incident using the Name, Number, Type, Host Unit, or Dispatch center. (This information is found on your resource order.) You may also scroll through the results box to find your incident
10. Click the Filter button
11. Click on your incident in the results box
12. Click the View Report button
13. With the report open click the Create ISUITE Extract button
14. Select a location to save your export file, and give it a desired name and set the Save As type to .txt (Text)
15. Click the save button

With the ROSS Import file in hand you may now import that data into your ISUITE database.

1. Open the Database Admin module on the SERVER computer
2. Click Import Data
3. Click the Browse button (…) on the right-side of the screen and navigate to where your ROSS import file is saved, select it and click OK
4. Click the load data button on the right-side of the screen

5. The Incident will appear in the left pane under ROSS Incident, Your ISUITE data will appear in the right-hand pane. Click the black arrow next to the ROSS incident to highlight it, and then click the black arrow next to the ISUITE incident to highlight it.
6. Click the Match button
7. Click Next
8. Click the double-headed arrow to move all of the ROSS resources from the import file to the ISUITE Resources pane
9. Click Next
10. You may need to repeat these steps for each resource type (aircraft, crews, equipment, overhead)
11. Once all of the resources from the ROSS import file have been moved to the ISUITE database you will receive a notification that the ROSS import is complete
12. Click OK
13. Close the ROSS Import window using the Red X at the top right corner of the window
14. Open the Resources Module to verify that resources have been imported to the database

*Please note: The ROSS import only populates limited fields for each resource under the Resources module. You will need to manually input the additional information.

*For additional information about performing ROSS imports please review the ISUITE User guides in the RESOURCES folder.

9. Database Back-ups:

The ISUITE application has several mechanisms to allow you to back-up database information. It is advised that after the initial set-up of a new Incident database or any time that a database is restored as part of a transition with another incident management team you enable the automatic back-up feature before you begin working in the database. This automatic back-up will be performed at intervals of 1 hour until it is disabled. The ISUITE backup feature allows you to specify any location you wish to store backup data. If possible it is recommended that you store backups on a machine other than your ISUITE server such as an external hard-drive. Additionally it is recommended that you perform manual backups at least daily and maintain them for your Incident package that is returned to the home unit. It is recommended that these manual back-up be created after creating the Injury / Finance data files that are to be uploaded to ISUITE.

To perform a manual ISUITE backup:

1. Open the Database Admin module
2. Click the Backup button
3. Ensure you are under the Manual Backup tab
4. Ensure that your Incident database is shown in the Database drop-down
5. The name box display the name that will be given to the backup file, leave it as the default (which is the database name, the date, and the time the backup is being preformed).
6. The Backup to box displays a location where the backup file will be saved
7. Click the browse button (…) to specify an alternate location or leave it as the default if you wish (The default location is c:\program files\isuite\database\backup).
8. Click OK
9. Click the Backup Now button
10. You will be notified that a Backup Is Now in Progress … Please Wait!
11. When your backup is complete Click OK

To set the automatic back-up schedule:

1. Open the Database Admin module
2. Click the Backup button
3. Select the Auto Backup tab
4. Check the box labeled Auto Backup Enabled
5. Check the box next to your database
6. Set the Backup Interval at 1 hour

7. Click the Browse button (…) to specify a Backup Destination or leave it as the default (The Default is C:\Program Files\ISUITE\Database\Backup)
8. Click the OK Button, then Save Button
9. Automatic Backups are now Set
10. Click the Close button

*Please note: Periodically the SERVER computer will display Backup In Progress… Please Wait!, during this operation will be unable to access the ISUITE application directly at the SERVER. Be patient, when the operation is complete you will be able to resume working.

10. Taking over an Incident:

If you are transitioning with another incident management team to take over an existing incident, the outgoing team will need to provide you with the most recent backup copy of the ISUITE database file, a username and password for a user that has Database Admin Rights, and the database password. To work with this database you will need to restore the database to your SERVER.

To Restore an ISUITE database:

1. Start your SERVER and Start the ISUITE application
2. Log-in as the Admin User
3. Navigate to the Database Admin module
4. Minimize ISUITE
5. Copy the database backup file to C:\Program Files\ISUUITE\Database\Backup (simply copy the file and paste it to the above folder.)
6. Maximize the ISUITE application
7. Click the Restore button
8. Click the Browse Button (…) and click on your backup file
9. The Restore As Database box is populated automatically
10. Enter the database password you were provided with
11. Click OK
12. The database will be attached automatically

*Please Note: Now that the database is restored and running please go in and set-up automatic backups for the database. For instructions on how to do this refer to page 14 of this guide.

You now need to go in and create your database users as they are shown in the Passwords file in the Resources folder. Refer to Page 17 of this guide to create users.

11. Database Users:

ISUITE requires that each user has a unique username and password combination to access a database. Your databases have been preset with a list of users for your team; please see the Passwords file in the Resources folder. If for some reason (i.e.: restoring a database from another team) you find the users specified in the Password do not exist you can enter them manually to ensure consistency.

To Create Users:

1. Open the Database Admin module
2. Click the Users Button
3. From this screen you can perform all Users Account Operations (Add / Delete Users, Activate / Deactive Users, Reset User Passwords, Modify a users rights, etc...) To add a new user
4. Click the Add button
5. Enter a User name
6. Enter a First Name
7. Enter a Last name
8. Enter the Temp password (see Password file) in the password box

*Please note the temp password is used when a new user is created in order to allow the user to login for the first time. After that first login you will be forced to reset the password.

9. Enter the Temp password (see Password file) in the verify password box
10. Click the Active check box to set the account as active

*Please Note: If the user is not set as active you will not be able to login to the account

11. Click the All Rights button on the right-side of the screen. (This will grant the user all the rights to the Database except Injury / Illness)
12. Click the Injury / Illness check box
13. Click the Save Button
14. Click OK
15. Note the User is added

*Please Note: It is advised that you setup your ISUITE databases to match the information in the Passwords file. It is recommended that you deactive any users in the database that are not shown in the Passwords file for consistency.

To Deactivate Users:

1. Navigate to the Database Admin module

2. Click the Users Button
3. Click the user you wish to deactivate to highlight it
4. Click the Active checkbox to uncheck it
5. Click the Save button
6. Click OK

To Change User Passwords:

1. Navigate to the Database Admin module
2. Click the Users Button
3. Click the user you wish to change to highlight it
4. Enter the new password in the Password box
5. Enter the new password in the Verify Password box
6. Click the Save button
7. Click OK

*Please Note: ISUITE security policy requires that passwords be changed every 60 days. Please be sure that if you make password or database password changes please be sure to note these changes in your passwords to the Passwords file.

12. Transitioning an Incident:

In a situation where you need to transition an incident to another incident management team you will need to provide the incoming team with a user name and password of an admin user to access the database as well as a most recent copy of the database backup file and the database password. For information on creating database backup see page 14 of this guide.

It is advisable to put the username and password information and the database password into a text (.txt) file. Copy that file, as well as the database backup file, along with any other important electronic information, to a CD-R or thumb drive for the incoming team.

Once the incoming team is set-up and running it is important to clean-your server computer and remove any unnecessary information. This has 3 benefits: it eliminates the confusion of having duplicate information; it protects PII; and it allows you to keep your SERVER more organized.

For Cleanup instructions see page 20 of this guide.

13. Cleaning Up the Server:

Once you have either closed out or transitioned the Incident to another incident management team or the home unit you will need to remove certain information from your server computer to prepare it for the next incident.

To Detach a Database:

1. Navigate to the Database Admin Module
2. Click the Detach button
3. Enter the database password
4. Click OK
5. You will note that the database is now detached and is no longer listed in the left pane

*Please Note: If you receive a warning that there are other users actively connected to the database only continue to detach it if you are sure no one is still working in it.

With your database detached it is now safe to go in and delete the actual database files and backups from the SERVER. Only proceed with this step if you are sure that the incoming team or home unit is up and running or has what they need to access the database information.

Deleting database files / backups:

1. Navigate to c:\program files\isuite\database
2. Delete all files **EXCEPT** for the following files: Masterdb2009!.mdf.gpg, ISuiteBlank, ISuiteMSDE.adp and dsn. Do not delete "Backup" folder, but delete the files in the Backup Folder.

*Please Note: If you have configured your SERVER to backup the database to another location, such as an external hard drive; be sure to delete the backup files from that location as well.

3. Go into the Shared Team Folder and delete any unneeded information from that location
4. Delete all export files in c:\program files\isuite\Data Export (delete files inside the 3 folders, but not the folders)
5. Delete any other incident specific files in other locations such as the desktops of the team computers, thumb-drives or non-team computers. This includes things like weather reports, ROSS import files or temporary notes.

*Please Note: Be cautious when deleting any files or information that may be important for documentation. Be sure all documentation has been turned over to an incoming team or the

home unit. Be sure this information is printed and / or saved electronically to CD-R and in the documentation folder of the final incident package

14. Module Basics:

RESOURCES Module:

Add / Edit Resources
Set Check-In Status
Enter Contractor Information
Enter Cost Info
Track Demob Information
Information in 'Resources' is used throughout the rest of the ISUITE application

IAP Module:

Used to prepare Incident Action Plan
One IAP for every operational shift
Forms may be copied from shift to shift making only required adjustments
Must identify operational periods
Must create a Master Frequency List
Be sure to Mark documents as Final and Lock them to ensure no additional edits are made. (They may be unlocked if necessary)

TIME Module:

Cost Tab in RESOURCES module must be filled out before you can enter time
Employee Type must be set in RESOURCES tab before you can enter time
Enter time worked to create pay documents for employees and contractors
Enter Actual Cost data for incident replacing cost estimates
Track Work / Rest ratio
Track lost work time
Allows posting of Additions / Deductions to invoice and or timesheets

COST Module:

Tracks Incident Cost
Perform Cost Analysis
Cost information used in the ICS 209 and documentation
Provides information for management Support and planning
Daily Accruals Sent to ISUITE
Provides Cost Projections
Allows you to manually edit or update incident cost information

REPORTS Module:

ISUITE has a wide variety of Graphs and reports related to all of its various modules. (Plans, Cost, Demob, Time, Injury/Illness)
It is possible to create custom reports using report designer or SQL statements in advanced designer
Reports can be saved and reused
ISUITE also has a quick stats function to provide real-time information about resources and their status
Reports are used as incident documentation, for tracking and planning purposes, and as a means of distributing information

15 . Plans:

Check In:

After the initial ROSS import resources are entered into ISUITE by Plans section through the check-in process. This is very important because the information provided during check-in is used throughout ISUITE in all the other modules. In the Type 3 folder you will find the ISUITE Check-In form that will allow personnel to provide all of the needed check-in information. Capturing all of this data accurately is important to the proper functioning of the ISUITE application and the quality of the products it produces for the incident. Certain information found in the Resources Module will need to be entered by the Finance section especially if the resource is an AD or under a Contract or EERA. During check-in please be sure to have these types of resources report to the Finance section so they can complete the process necessary to capture copies of this documentation.

There are a number of important documents and / or pieces of information that need to be collected during the check-in process. Be sure to collect Resource Orders, Contracts, EERA's, manifests, and rosters.

Other information that is needed during check-in includes:

- Travel Arrangements
- Home Unit Info
- Last Day Off
- Days on Previous Fire Assignment
- Other Red Card Quals
- Work / Rest / Travel Time
- Capture Engine Number (not resource E#)
- Number of People (corrections to manifest)

For more Information See the ISUITE USERGUIDE.

Demob:

As resources are released from the incident, either to their home unit or to another incident, they must follow the demob process. This process allows the Plans section to develop tentative demob plans daily and notify dispatch of resources being released. This allows dispatch to attempt to reassign resources to other incidents or to scale back their operations appropriately. During demob the Plans section will ensure proper check-out procedures are followed with all

sections (Logistics, Finance, Plans), track resources for reassignments, make travel arrangements if necessary, and notify dispatch of departure and eta to next stop as resources are released from the incident. ISUITES' DEMOB Module can be used to track resources, plan the demob process, and to generate reports and documentation related to the demob process. For more Information See the ISUITE USERGUIDE.

IAP:

The plans section is responsible for generating an Incident Action Plan for every shift on an incident. The IAP module in the ISUITE application allows you to create and modify the various forms included in the IAP. These forms can then be modified and reused to create future IAP documents with only necessary edits. Before creating an IAP you need to define incident shifts and create a master frequency plan. With this information complete you can create the various forms necessary to complete the plan.

There are several types of documents commonly used as part of the IAP that are not created in ISUITE. These include;

Cover Sheets
Maps
Weather Information
Safety Messages

Copies of the IAPs for each shift should be included in the incident package. For more Information See the ISUITE USERGUIDE.

ICS 209

The Incident Status Summary is a report that is to be submitted to the incident dispatch center daily, or sometimes twice a daily. This information is used in the planning and prioritizing of resources, as well as for reporting of incident status and cost. Information for incident 209's is also used to generate the Interagency Sit Report and for reporting to managers and agency administrators. This information can be reported electronically through the FAM Web application, submitted to dispatch via hardcopy, email, or fax, or reported to dispatch via radio or telephone. For more information see http://fam.nwcg.gov/fam-web/

16. **Finance Section:**

Resources Module:

The Finance section will need to enter various pieces of information in the resources module that are used to generate pay documents and cost information and reports. Under the resources module resources can be identified as contracted resources by clicking the contracted checkbox. This includes tactical resources (engines, dozers), support or camp equipment (showers, generators), and contract crews. If a resource is hired under EERA or some other type of agreement the time – contracted tab will appear in the Resources module. Under this tab the Finance section will need to enter the contractor information, agreement information, admin office for payment information, and the various rate types used to compensate the resource based on their contract or EERA. No time may be input for a contractor until this information is complete.

If the resource is identified as a person by clicking the person checkbox in the Resources tab the time-individual tab will appear. Under this tab the finance section will need to classify the person as being a federal employee (FED), a casual hire (AD), or employed outside of the federal government (Other). Various different types of information are needed based on each of these selections. In the case of AD personnel there is additional information needed for these employees. This information applies to single resources, members of a crew, or crew members attached to equipment or aircraft. No time may be input until this information is complete.

Each resource assigned to an incident has a Cost tab under the Resources Module. The Finance Section needs to complete this information to ensure the accuracy and completeness of the COST data. By default ISUITE generates a daily cost for every resource assigned to the incident. This may or may not be appropriate, please review this information for accuracy. For more Information See the ISUITE USERGUIDE.

TIME MODULE:

The time module is used by the Finance Section to input hours of work for people and equipment. This includes single resource personnel, Hand crews, engine crews, aircraft crews, and any equipment used on the incident. This information is captured from signed CTR's or Equipment Shift Tickets. Additionally travel time is input for both personnel and equipment. Regular federal employees may also be entitled to Hazard Pay if certain work conditions are met. This information is also input into the time module.

Both personnel and equipment may be entitled to additions or deductions to their pay documents in certain circumstances. Deductions would be for expenses to the incident not paid for under agreement. Examples would be things like fuel or commissary purchases. Additions, on the other hand, are for cost incurred to the contractor or employees that are reimbursable by the incident. Examples would be things like Cell phone usage, or the settlement of a claim for damage or loss.

For every resource being paid by the incident either CTR's, Equipment Shift Tickets, or both need to be kept as documentation for every resource for the final incident package. Additionally a copy of the resource order for every resource on the incident is required. Based on the resource type and / or the conditions of Hire various types of additional documentation may be need to be included with the pay documents. Contractors are required to have a copy of their contracts or EERA's and equipment use inspections. AD employees also need a copy of their Casual hire form and I9 as part of their payment documentation. For more information see the ISUITE USERGUIDE and the IIBMH.

Finalizing Time:

As part of the demob process the Finance section will finalize personnel time in ISUITE. Please review all postings and ensure that all CTR's are posted correctly. Verify that hazard pay is posted if applicable. Open a column for return travel and have employee review for accuracy. Print the final document and obtain signatures. In most cases the employee will get the original and the incident will maintain a copy, except in the case of FS AD employees, the incident will submit the original for payment and make 2 copies -one for the incident package and one for the AD employees' records. The general rule of thumb is that originals must be used to send into the payment center. For more information see the ISUITE USERGUIDE and the IIBMH.

As part of the demob process for contractors the Finance Section will finalize equipment time in ISUITE. Please review all posting and ensure the all shift tickets are posted correctly. Verify that all rates are correct and that any additions or deductions are posted if applicable. Estimate travel time home and have contractor review for accuracy. Print the final document and obtain signatures. The incident will submit the original invoice for payment and make two additional copies, one for the incident package and one for the contractors records. Ensure that all equipment / contract packets are complete before the contractor leaves the incident. The general rule of thumb is that originals must be used to send into the payment center. For more information see the ISUITE USERGUIDE and the IIBMH.

COST

The ISUITE cost module allows the Finance Section to track incident costs as well as perform cost analysis and projections. This information is used in management support and planning. Additionally this information is used in reporting via the ICS 209 and COST information has to be uploaded daily.

By default every resource in the ISUITE database will roll-up an estimated daily cost. Performing the cost run at intervals from the COST module will replace these estimated cost with the actual cost input via the TIME module and additionally incident costs can be entered directly from the COST module. Daily COST summaries are required as part of the final incident package. ISUITE offers a wide range of available cost reports and graphs. In addition custom reports can be created within the ISUITE application. For more information see the ISUITE USERGUIDE and the IIBMH.

17. ISUITE REPORTS:

The ISUITE application includes a wide variety of Graphs and reports for each of its various modules (Plans, Cost, Demob, Time, and Injury Illness). It is also possible to create custom reports using report designer or SQL statements in the advanced reports designer. Any custom reports that are created can be saved and reused at a later date.

In addition to the reports ISUITE has a quick stats function to provide real-time information about resources and their status with a single click. This function provides information such as number of personnel on incident, or number and type of engines currently assigned. These functions provide an easy way to compile data and present it easily. For more information see the ISUITE USERGUIDE.

18. Daily Exports:

Certain pieces of information generated within the ISUITE application are required to be uploaded on a daily basis from the incident. This information includes the incident COST accrual information as well as injury / illness information. During the export process the ISUITE application will create export files for this information that will then need to be uploaded to the ISUITE data repository at:
https://isuite.nwcg.gov/Repository/index.html
*Please Note: All Incident management teams are required to upload this information daily.

To generate export files:

1. Open The Database Admin Module
2. Click the Export Data button
3. Use the radio buttons on the left of the screen to select the export type (financial, injury/illness, repository)

*Please Note: For information on creating a repository file see the database repository section on page 32 of this guide

4. Use the dropdown menu to select the database to export from
5. Use the dropdown menu to select the incident to export from
6. Click OK
7. You will be notified that after data has been exported it will be locked. Click OK
8. After your export file is shown in the export history pane it is ready to be uploaded. Close the Data Export window by clicking the Close Button or the X at the top right corner of the window.

After the export files are created they are saved to c:\program files\isuite\Data_Export. Under this export directory there are a number of other folders for each of the various types of export files created. The Finance file is where all of the financial accrual data files will be stored. The Other folder is the file where all of the injury/illness export files will be stored. The Repository folder is where all of the Database repository files will be stored. If the SERVER does not have an internet connection you may need to copy these export files to a CD-R or a thumb drive to move them to a computer that can access the ISUITE website to perform the upload.

You will note that for each export that is created there will be 2 files a cce.gpg file and a xml.gpg file, both of these files need to be uploaded to ISUITE. The file names are the incident number, the date, and the time. Please do not modify these names, this naming convention is needed in order to upload the information properly.

To perform the upload:

1. Navigate to https://isuite.nwcg.gov/Repository/index.html
2. Enter the Username and Password of the repository user (see passwords file)
3. Click OK
4. Click the Browse Button
5. Navigate to the location of your export file either located on the SERVER or your thumb drive CDR etc…

*Please Note: Do not modify the name generated from the ISUITE application when uploading files.

6. Click the Upload! Button

*Please Note: Each of the various export files needs to be uploaded separately by clicking the back button to return to the upload screen. Repeat the steps above to complete all of the uploads.

7. You will be notified that your files were saved
8. You can close the window

For more information see the ISUITE USERGUIDE.

19. CLOSING OUT AN INCIDENT

If the incident is being closed out, meaning that there are no resources assigned to the incident, or it has transitioned to a Type 4 organization, there are certain procedures that need to be followed.

First, if there are to be no resources assigned to the fire:

1. Open the data admin module
2. Click on the incident to highlight it
3. Enter the end date
4. Click the Save button
5. Click OK

*Please Note: DO NOT enter an end date if there are still resources assigned to the fire.

6. Continue to close-out checklist.

If there are resources still assigned to the incident and or it is being transitioned to a type 4 incident continue to the close-out checklist.

CLOSE OUT CHECKLIST:

1. Close out and demob all resources that are no longer on the incident
2. Perform a final cost run and generate any needed reports
3. Create and upload any final export files for the incident (see page 29 of this guide)
4. Perform a final database backup (see page 14 of this guide)
5. Create and upload the database repository file (see page 32 of this guide)
6. Burn the ISUITE backup file, username, password and database password text file, and any other important electronic data to a CD-R for the final incident package
7. Perform the SERVER clean-up steps (see page 20 of this guide)

20. Database Repository

There are two cases when you may want to create an ISUITE repository file. First, if all incident resources have been demobed from the incident and it is being turned over to the home unit. Second, if the incident is being transitioned to a smaller command organization such as a type 4. It is likely that this smaller organization will no longer be using ISUITE to track incident data. In a case where you are turning the incident over to a larger organization (Type 1 or Type 2) you do not need to create a repository file.

If you are handing the incident over to a type 4 organization it is advisable to check-in the initial resources that will be used in that new organization and show them as assigned to the incident before you create a repository file. Be cautious to only create a repository file when you are certain that all of the work that needs to be completed in the database is finished. All resources no longer assigned to the incident need to be closed out and demobed. All the final reports and database uploads need to be completed.

To create a repository file:

1. Open the Database Admin Module
2. Click the Purge SSN/EIN button

*Please Note: this will set all the EIN SSN numbers to 9's in the database and erase PII data.

3. Click Yes
4. Click Yes
5. Click OK
6. Click the Export Data button
7. Set the Export Type as Repository
8. Select your database from the drop-down
9. Select your incident for the drop-down
10. Click OK
11. You will notified that after data has been exported it will be locked. Click OK
12. After your export file is shown in the export history pane it is ready to be uploaded. Close the Data Export window by clicking the Close Button or the X at the top right corner of the window.
13. Your file will be saved in c:\program files\isuite\data_export\repository using the naming convention of Incident number, date, and time. Please do not rename this file. The naming convention created in ISUITE is needed for the information to upload properly.
14. You will need to upload this file to the ISUITE Data Repository at https://isuite.nwcg.gov/repository/index.html. For information on how to do this see page 29 if this guide.

21. MORE INFORMATION:

- Review I-Suite Training Material http://isuite.nwcg.gov/training/index.html
- Click 'Help' in the I-Suite application
- Review I-Suite User guides and Quick Start Guide guides in the 'Resources' folder
- Review the information on the ISUITE website http://isuite.nwcg.gov